

### Claims

1. A device for secure access to digital media contents, the device comprising an access means for accessing digital media contents from a data source and a  
5 reader for authenticating a user, the authentication being performed by checking some authentication data, characterized by an internal communication path between the access means and the reader which is not directly accessible from outside the device.
2. The device according to claim 1, characterized in that the device only has a  
10 single electrical interface for connection to a host.
3. The device according to claim 2, characterized in that the single electrical interface represents at least two logical interfaces, a first logical interface being compatible to the digital media and a second logical interface being compatible to the authentication data.
- 15 4. The device according to claim 3, characterized in that the single electrical interface is designed according to one of the following standards: USB, SCSI, Firewire, PCMCIA, WiFi, Bluetooth, HyperLAN.
5. The device according to any of the preceding claims, characterized in that the access means and the reader share a common processing unit.
- 20 6. The device according to any of claims 1 to 4, characterized in that the access means and the reader use different processing units, the communication path including a communication channel between the processing units.
7. The device according to any of the preceding claims, characterized in that the access means and the reader are accommodated in a single housing.
- 25 8. The device according to any of the preceding claims, characterized in that the reader is a smart card reader capable of accessing a key stored on a smart card.

9. The device according to claim 8, characterized in that the device comprises means for entering a PIN code and is capable of releasing the key after a PIN code match is determined.

10. The device according to claim 8 or 9, characterized in that the smart card  
5 containing the key is interfaced to the smart card reader through one of the following interfaces: ISO 7816, I2C, Contactless Smart Card Interface.

11. The device according to any of claims 8 to 10, characterized in that the smart card is embedded inside the reader.

12. The device according to any of claims 1 to 7, characterized in that the  
10 reader is capable of retrieving biometric information from the user.

13. The device according to claim 12, characterized in that the reader includes one of the following: a fingerprint sensor, an iris recognition means, a face recognition means, a voice recognition means.

14. The device according to any of the preceding claims, characterized in that  
15 the data source is one of the following: a hard disk, a removable disk, a CD, a DVD, a flash memory embedded inside the device, a removable flash memory.

15. The device according to any of claims 1 to 13, characterized in that the access means includes a modem capable of retrieving data from a remote network, especially from the internet.

20 16. The device according to any of the preceding claims, characterized in that at least one of the access means and the reader is a module which can be inserted into and removed from the device.

17. The device according to any of claims 1 to 15, characterized in that at least  
25 one of the access means and the reader is a system-on-chip (SOC) or a single chip system.

18. A virtual multi-interface driver for supporting a device having at least two device functions and being connectable to a host via a single electrical interface, characterized in that the virtual multi-interface driver reports at least two logical interfaces to the system software of the host, in the logical interfaces including at  
5 least one virtual interface in addition to the single electrical interface.

19. The virtual multi-interface driver according to claim 18, characterized in that the virtual multi-interface driver is capable of switching between the two logical interfaces in response to a switch command.

20. The virtual multi-interface driver according to claim 18 or 19,  
10 characterized in that the virtual multi-interface driver creates a virtual user authentication interface.

21. The virtual multi-interface driver according to any of claims 18 to 20, characterized in that the virtual multi-interface driver converts commands received from the operating system of the host into a format compatible with the  
15 single electrical interface.

22. The virtual multi-interface driver according to claim 21, characterized in that the virtual multi-interface driver converts commands from a smart card command format into an SCSI command format.

23. The virtual multi-interface driver according to any of claims 18 to 22,  
20 characterized in that the virtual multi-interface driver reports  $n-1$  virtual interfaces to the system software of the host, with  $n$  being the number of device functions.

24. A system for secure access to digital media contents, the system comprising a device according to any of claims 1 to 17, a virtual multi-interface driver according to any of claims 18 to 23 and a host.

25. The system according to claim 24, characterized in that the device is  
25 connected to the host via a single electrical interface provided on the device, thus only a single data channel being provided for communication between the device and the host.

26. The system according to claim 24 or 25, characterized in that the virtual multi-interface driver acts as an interface between the drivers of the access means and of the reader, which are loaded by the system software of the host, on the one side and the single electrical interface of the device on the other side.

- 5        27. The system according to any of claims 24 to 26, characterized in that the host comprises means for entering a PIN code, the PIN code or a derivative thereof being communicated to the device via the single data channel.

28. The system according to any of claims 24 to 27, characterized in that the device is accommodated inside the host.

- 10       29. The system according to any of claims 24 to 27, characterized in that the device is an external unit remote from the host.

30. The system according to any of claims 24 to 29, characterized in that the device comprises a plurality of device functions, the virtual multi-interface driver reporting n-1 virtual interfaces to the system software of the host, with n being the  
15       number of device functions provided in the device.